

IN THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the Application:

LISTING OF CLAIMS:

1. (Currently Amended) A dynamic file access control and management system configured to access one or more content sources, including a set of content, said system comprising:

- A. a proxy system linked to said one or more content sources, said proxy system comprising an access control module configured to selectively obtain content comprising data blocks from said content sources on an individual block basis as a function of an authorization of a user requesting said content and a set of access policies comprising a set of predefined usage policies associated with said content for said user;
- B. a rights management module configured to generate a set of usage rights associated with said content as a function of the set of predefined usage policies associated with said content for said user;
- C. at least one client device having a client module configured to interface to a client operating system kernel, said client module configured to enforce the set of usage rights within the operating system kernel without application rewrites, wherein enforcing the set of usage rights within the operating system kernel includes:

- intercepting a system call between an application and the client operating system;
  - evaluating the system call based on the set of usage rights;
  - and
  - blocking or modifying the system call based on said evaluation; and

D. one or more communication means, via which said content and said usage rights are provided to said client device;

wherein selectively obtaining content comprising data blocks from said content sources on an individual block basis includes:

obtaining data blocks from said content sources, each data block being of a fixed preconfigured size, said fixed preconfigured size being associated with said content and stored on said content sources; and

obtaining the fixed preconfigured size associated with said content from said content sources.

2. (Previously Presented) The system according to claim 1, wherein said content and said usage rights are provided to said client device via different communication means.

3. (Previously Presented) The system according to claim 1, wherein said content includes static content.

4. (Previously Presented) The system according to claim 1, wherein said content includes dynamic content.

5. (Previously Presented) The system according to claim 1, wherein said communication means includes a secure transform configured to encrypt and encapsulate said content into a message as a function of a session ID and said client is configured to extract said content from said message.

6. (Previously Presented) The system according to claim 1, wherein said proxy system further includes a user interface, configured to facilitate creation and editing of said access policies and said usage policies and association of said access policies and said usage policies with said content.

7. (Previously Presented) The system as in claim 1, wherein said client device is a device from a group comprising:

- 1) a personal computer;
- 2) a workstation;
- 3) a personal digital assistant;
- 4) an e-mail device;
- 5) a cellular telephone;
- 6) a Web enabled appliance; and
- 7) a server.

8. (Original) The system of claim 1, wherein said proxy system and at least one of said content sources are hosted on the same computing device.

9. (Currently Amended) A method of dynamic access control and management of content, the method comprising:

- A. to content comprising data blocks accessible from a set of content sources on an individual block basis as a function of an authorization of a user requesting said content and a set of access policies comprising a set of predefined usage policies associated with said content for said user by a proxy system, correlating one or more user and/or client device identifications and defining the set of usage policies, wherein for the content said usage policies relate to selectively enabling or disabling operations associated with said content;
- B. by said proxy system, generating a set of usage rights associated with the content as a function of the set of usage policies associated with said content and the one or more user and/or client device identification;
- C. communicating said content and said usage rights to a client device associated with said one or more user and/or client device identification; and

D. using a client module at said client device and configured to interface to a client operating system kernel without application rewrites, enforcing the set of usage rights within the operating system kernel, wherein enforcing the set of usage rights within the operating system kernel includes:

intercepting a system call between an application and the client operating system;

evaluating the system call based on the set of usage rights;  
and

blocking or modifying the system call based on said evaluation;

wherein the content comprising data blocks includes data blocks having a fixed preconfigured size associated with said content, said fixed preconfigured size being stored on said content sources; and the method further comprises:

obtaining the fixed preconfigured size associated with said content from said content sources.

10. (Previously Presented) The method of claim 9, wherein in step C, said communicating is accomplished by communicating said content and said usage rights to said client device via different communication means.

11. (Previously Presented) The method of claim 9, wherein said content includes static content.

12. (Previously Presented) The method of claim 9, wherein said content includes dynamic content.

13. (Previously Presented) The method of claim 9, wherein said communicating is accomplished using a communication means that includes a secure transform, including encrypting and encapsulating said content into a message as a function

of a session ID and said client device is configured to extract said content from said message.

14. (Previously Presented) The method of claim 9, wherein said proxy system further includes a user interface and step A include creating and/or editing said access policies and said usage policies and associating said access policies and said usage policies with said content using said user interface.

15. (Previously Presented) The method of claim 9, wherein said client device is a device from a group comprising:

- 1) a personal computer;
- 2) a workstation;
- 3) a personal digital assistant;
- 4) an e-mail device;
- 5) a cellular telephone;
- 6) a Web enabled appliance; and
- 7) a server.

16. (Previously Presented) The method of claim 9, further comprising hosting said proxy system and at least one content source on the same computing device.

17. (Previously Presented) The system according to claim 1:

wherein the access control module is further configured to encrypt each data block of the content independently, using a unique initialization vector for each data block and one or more encryption/decryption keys; and

wherein the one or more communication means also provide the one or more encryption/decryption keys to said client device.

18. (Previously Presented) The system according to claim 1 wherein each content source stores a plurality of directories, at least one directory including a plurality of content files and a metafile, wherein the metafile stores a plurality of records, each record corresponding to one of the plurality of content files within that directory, each record storing the set of predefined usage policies associated with the corresponding content file.

19. (Previously Presented) The method of claim 9 wherein the method further comprises:

encrypting each data block of the content independently, using a unique initialization vector for each data block and one or more encryption/decryption keys; and

communicating said one or more encryption/decryption keys to said client device associated with said one or more user and/or client device identification.

20. (New) A method performed by a proxy server, the method comprising:

receiving, over a first network connection, a Network File System (NFS) based request from a client machine for a data block of a data file from a remote network attached storage system, the request having an associated user, the data block having a fixed preconfigured size associated with the data file;

requesting, from an authentication server, an access policy associated with the associated user;

receiving, from the authentication server, the access policy associated with the associated user;

determining, from the access policy associated with the associated user and metadata associated with the data file, the metadata being stored on the remote network attached storage system, if the associated user has the authority to access the data file; and

if the associated user has the authority to access the data file, then:

establishing a set of usage rights based on the access policy associated with the associated user and the metadata associated with the data file;

requesting, over a second network connection, from the network attached storage system, the data block of the data file;

receiving, over the second network connection, from the network attached storage system, the data block of the data file;

encrypting the received data block, such that only an authorized client module executing on the client machine by the associated user can decrypt the encrypted received data block;

encapsulating within a packet:

the encrypted received data block; and

the established set of usage rights; and

sending, over a secure channel, the packet to the client machine such that only the authorized client module can access the encrypted received data block and only when such access is in accordance with the established set of usage rights, said authorized client module running transparently to the associated user, logically interposed between an application layer and an operating system kernel layer.

21. (New) A method as in claim 20 wherein the established set of usage rights includes one or more access restrictions, each usage restriction including:

a restriction type; and

a set of parameters associated with the restriction type.

22. (New) A method as in claim 21 wherein the restriction type indicates that data from the encrypted received data block may only be e-mailed to recipients listed within the set of parameters.

23. (New) A method as in claim 20 wherein the access policy associated with the associated user includes a set of access conditions, each access condition including:

- a condition type; and
- a set of parameters associated with the condition type.

24. (New) A method as in claim 23 wherein the condition type indicates that the associated user only has the authority to access the data file when the clock time falls between a first value listed in a first parameter of the set of parameters and a second value listed in a second parameter of the set of parameters.